International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

LHC: Secure and Efficient Hybrid Cloud Base Firewall policy for Data Confidentiality

Mr. Venkanna. B & Dr. Ravisankar Malladi

[1]Department of CSE,Vaagdevi Engineering College,Bollikunta, Warangal-506 005,Telangana,India

[2],Department of CSE,Vaagdevi College of Engineering(Autonomous),Bollikunta,Warangal - 506 005,Telangana,India

Abstract: -*As the cloud computing paradigm evolves; new types of cloud-based services have become available, including security services. Some of the most important and most commonly adopted security services are firewall services. These cannot be easily deployed in a cloud, however, because of a lack of mechanisms preserving firewall policy confidentiality. Even if they were provided, the customer traffic flowing through the Cloud Service Provider infrastructure would still be exposed to eavesdropping and information gaining by performing analysis. To bypass these issues, the following article introduces a novel framework, known as the Ladon Hybrid Cloud, for preserving cloud-based firewall policy confidentiality. It is shown that in this framework, a high level of privacy is provided thanks to leveraging an anonymized firewall approach and a hybrid cloud model. A number of optimization techniques, which help to further improve the Ladon Hybrid Cloud privacy level, are also introduced. Finally, analysis performed on the framework shows that it is possible to find a trade-off between the Ladon Hybrid Cloud privacy level, its congestion probability, and efficiency. This argument has been demonstrated through the results of conducted experiments.*

Keywords:- **Firewall , Cloud computing , Privacy , Bloom Filter.**

INTRODUCTION

During the past couple of years, the cloud computing paradigm has evolved from an experimental approach to hosting Information and Communications Technology (ICT) services in a distributed systems environment, to a leading trend in the ICT market. Thanks to this, most types of services are available in a cloud today, including security services. The model of hosting security services in a cloud is referred to as Security as a Service (SecaaS). Following the needs of business which keep increasing due to the expansion of the technology, many ICT companies, including leaders such as AT&T with itsNetwork-Based FireWall Services(NBFWS) [3], have already begun offering security services in a cloud. These include firewall services, Intrusion Prevention System (IPS) services, e-mail filtering, and web filtering. In most cases, including AT&T NBFWS and Cloud era Enterprise Services Cloud (ESC), the security services are deployed by leveraging a hybrid cloud model with customers connected to the Cloud Service Provider (CSP) via a secure Virtual Private Network (VPN) connection.

In such a system, most of the customer security services are hosted in a cloud, while the basic security infrastructure, responding to last mile attacks for example, remains on its premises. The on-premises infrastructure can be managed by the CSP or the customer. Alternatively, a hybrid management system can be applied with the CSP being responsible for the on-premises infrastructure installation, its initial configuration, monitoring, etc., and the customer being responsible for the entire security policy management. One of the core security services adopted by the vast majority of organizations are firewall services. It is hard to imagine an enterprise, government unit, university, or even home business running its network services without being protected by a firewall. Thanks to such technologies as AT&T NBFWS or Virtela ESC, these can be outsourced to the cloud, resulting in significantly reduced management overhead, decreased Total Cost of Ownership (TCO), improved business agility. However, because of a lack of mechanisms preventing the CSP from having an insight into the customer' firewall policy, there are still issues of information confidentiality and privacy.

In addition, another threat is information gaining by traffic eavesdropping and analysis. Since in a hybrid cloud SecaaS model all the traffic flows unencrypted through the CSP infrastructure and there are no mechanisms protecting against eavesdropping, sensitive information such as that regarding allowed Internet Protocol (IP) addresses can be easily gained by the CSP based on traffic analysis. This exposes a serious vulnerability of such systems, as according to recent reports, most data harvesting events take place during transit.

RELATED WORK

TheLadon framework as a first step toward cloud-based firewalling. The Ladon leverages an anonymized firewall based on a set of Bloom Filter Firewall Decision Diagrams (BFFDDs) which are compiled from regular Firewall Decision Diagrams (FDDs) in which edge sets are replaced by Bloom Filters (BFs). Thanks to the merging of these elements that are explained in detail in the next section, regular Access Control List (ACL) rules are transformed into a structure which is still visible to the CSP, although it does not provide it with straightforward information regarding the original ACL structure. In such a framework, the ACL rules of the customer's firewall can neither be directly read by the CSP, nor easily cracked using brute-force techniques. However, as described below, these can be determined by packets eavesdropping and analysis. Other studies related to the topic of this article are those related to moving target defense.

Theauthors have studied techniques of substituting different targets for any given request in order to create a dynamic and uncertain attack surface area of a given system. This enabled them to demonstrate that such systems are less vulnerable and more secure. The Ladon Hybrid Cloud framework presented in this article also intentionally introduces uncertainty to the attack surface area; however, it achieves this by using a BF false-positive rate, as explained below. All targets remain unchanged for all given requests over time.

FROM ACL TO LADON

An FDD, presented by Gouda and Liu, is a mathematical structure which is a formal firewall representation. In fact, the FDD transforms a regular firewall policy based on a set of Access Control Entry (ACEs) into a tree where packets pass from top to bottom, with particular packet fields being examined at each level. Depending on its particular packet field value, the packet is directed to one of the edges, forming a decision path which finally takes one of the two possible decisions: permit or deny.

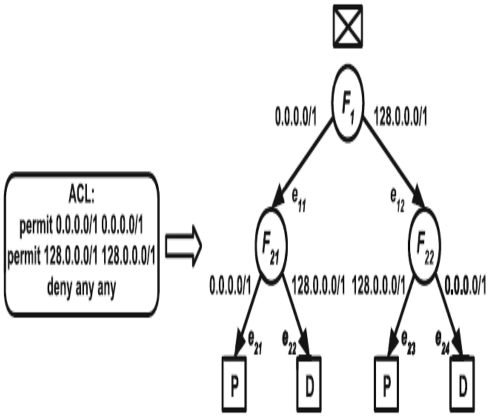

Fig. 1 FDD construction

This concept is shown in Fig. 1. Suppose that the firewall takes its final decision based on the source and destination IP addresses alone. The FDD then consists of two levels: one representing the source IP address and the other representing the destination IP address. The edge sets are calculated based on the corresponding ACL. For example, for a packet sourced at 10.10.10.10 and destined for 192.168.192.168, which fits the first ACE in the ACL, its source IP address is examined first on the F1 node. 10.10.10.10 fits the 0.0.0.0/1 set, so the packet is passed to the e11 edge, where its destination IP address is examined on the F21 node. Because 192.168.192.168 fits the 128.0.0.0/1 set, the packet is passed to the e22 edge, resulting in a deny decision.

Unlike in a regular firewall, where a packet is examined as a whole by testing it against ACEs from top to bottom until the first match is found, the FDD takes a completely different approach. It splits the packet into fields and examines each field independently on particular tree levels. The resulting path leads to a single, ultimate decision. Sample FDD implementation known as 'Policy Trie' was also presented independently of Gouda and Liu's work by Fulp and Tarsa in [18]. A BF, presented by Bloom in [16], is a mathematical probabilistic data structure which is used to test whether an object is a member of a set in a time-efficient manner. Mathematically, a BF is a bit array with a size of m which is generated by calculating k-independent hash functions for each of n elements of the set. For each of the results, the corresponding index in BF is set to 1. To check whether an element is a member of the original set, the same hash functions are calculated and corresponding indexes of the BF are checked. If at least one of them is 0, the element is not a member of the original set. If all of them are 1, the element may be a member of the original set. The above indicates that a BF may result in false positives. Moreover, the value of false-positive probability, also known as the BF false-positive rate, can be calculated based on the k, m, and n parameter [19].

So far, brick level structures which build up BFFDD have been covered. Based on them, the BFFDD definition can be explained as follows. According to [14], the BFFDD is a data structure formed from regular FDD where, for a given edge, the edge set is represented by a BF. Because it is in the nature of the BF that it may result in false positives, ambiguities may occur in BFFDD, leading to multiple decision paths and as a result to multiple decisions. To eliminate such ambiguities N, independent BFFDDs are implemented and executed simultaneously. The resulting decision paths are then compared looking for a single, common path which leads to a common, final decision.

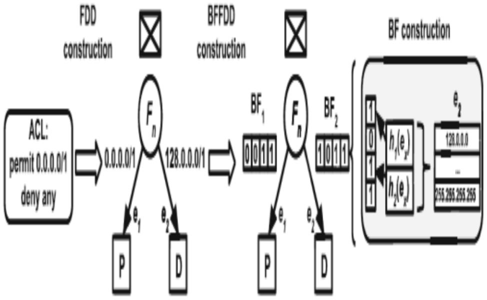

Fig.2 BFFDD construction

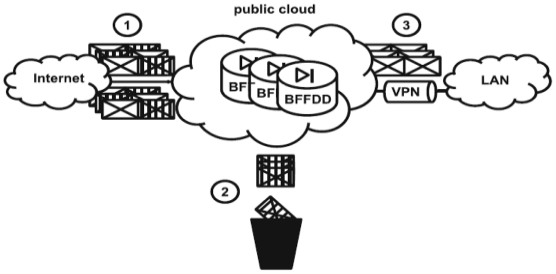

Fig. 3Ladon framework

The concept of BFFDD and its construction algorithm is shown in Fig. 3. Suppose that the firewall takes its final decision based on the source IP address only. The original ACL is then transformed into an FDD with one level only. Next, the edge sets e1(0.0.0.0/1) and e2(128.0.0.0/1) are transformed into BF1 and BF2 correspondingly. The process of BF2 construction is shown within the gray round rectangle. However, the BF shown in this example has a size of m = 4 and uses k = 2 hash functions; these are obviously much greater in a real scenario. Section 1 shows a standard business model for hosting firewall services in the cloud. Outsourced firewall services are hosted in the public cloud located in the data center owned and managed by the CSP. All traffic destined to the customer first enters the public cloud, which is connected with customer premises via a secure VPN connection. The technology used to deliver firewall services is not visible to the customer. Assume that it is based on a set of independent BFFDDs as described above.

A framework of cloud-based firewall services based on BFFDDs is shown in Fig. 4. Packets permitted on customer premises, referred to as 'good packets' in the rest of the article, are represented there by plain envelopes. In turn, packets denied on customer premises, referred to as 'bad packets' in the rest of the article, are represented there by striped envelopes. All packets enter the public cloud first (step 1) where bad packets are discarded (step 2). Next, good packets are sent to customer LAN (step 3). Such framework was referred to as the Ladon framework by its authors in [14]. By implementing and testing Ladon in a live environment, Khakpour and Liu demonstrated that it is an effective framework for the outsourcing of the firewall services. It was also shown that any attempts to de-anonymize the BFFDD can be extremely time-consuming.

LADON HYBRID CLOUD OPTIMIZATION

Although the BFFDD may result in multiple decisions for some of the packets, for the others, a final decision remains certain. Part of the knowledge base maintained by the hostile CSP will therefore always be accurate. It is possible to eliminate this vulnerability, however, by redesigning the BFFDD in such a way that it always results in multiple decisions for either good or bad packets, based on the adopted firewall policy type. In the real world, two types of firewall policies can be adopted based on organization requirements:

– Closed: Permitting only a specific subset of traffic and denying the rest,
– Open: Denying only a specific subset of traffic and permitting the rest.

For inbound traffic flow, considered in this article, most organizations apply the closed firewall policy rather than the open one, because it minimizes the risk of malicious traffic passing through. In such a case, the BFFDD is redesigned in such a way that it always results in multiple decisions for good packets. As closed firewall policy is a leading trend in most of the organizations today, it will be used as an example in further arguments in this article. Likewise, in an organization applying open firewall policy, the BFFDD can be redesigned so it always results in multiple decisions for bad packets accordingly. As has been mentioned, in the case of a closed firewall policy type, the

BFFDD is updated to always result in multiple decisions for good packets. The only packets that may still result in certain decisions are therefore bad packets. The framework is designed in this way, because when adopting closed firewall policy type, good packets carry significantly more information for the CSP regarding the original ACL structure compared to bad packets. This is because a characteristic of closed firewall policy type is that the subset of traffic which is permitted is much smaller than the subset of traffic which is denied. Figure 6 represents a BFFDD with one level and all the cases that it can result in:

– Case 1: Certain permit decision for good packets,
– Case 2: Multiple decisions for good packets,
– Case 3: Certain deny decision for bad packets,
– Case 4: Multiple decisions for bad packets.

As mentioned above, case 1 should be fully eliminated. To achieve this, a regular BFFDD is compiled first and then tested against all good packets. For those resulting in certain permit decisions (case 1), the BF representing the set of the edge that leads to a deny decision (BF2 in this case) is updated so that it results in a forced false positive.

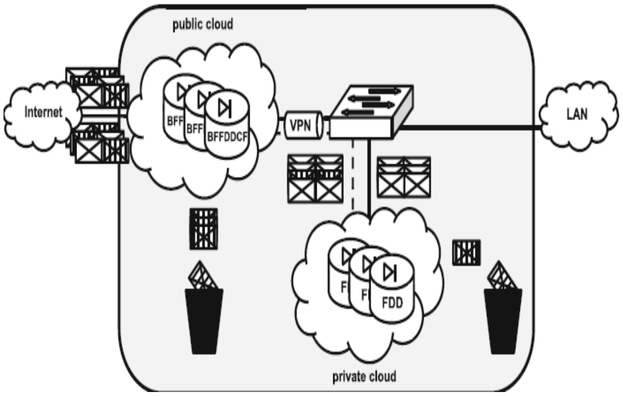

Fig. 5 closed firewalls

As a consequence, multiple decision paths are applied to all good packets (case 2) leading to multiple decisions applied to all of them. In other words, the redesigned BFFDD eliminates case 1 by transforming it into case 2, resulting in three possible cases (2, 3, and 4) shown inside the gray round rectangle. The above transformation can be performed on any BFFDD level; however, for analysis and implementation simplicity, it is assumed that it is performed on the last level representing the last examined packet field. Such a redesigned BFFDD will be referred to as BFFDDCF (Bloom Filter Firewall Decision Diagram for Closed Firewalls).

Likewise, such a redesigned Ladon Hybrid Cloud which leverages a BFFDDCF in a public cloud will be referred to as Ladon Hybrid Cloud for Closed Firewalls (LHCCF). As a consequence, the traffic flowing between public and private clouds consists of all good packets and some bad packets, while multiple decisions are applied to all of them by the BFFDDCF. This leads to a situation where all packets flowing between the CSP and the customer go via an untrusted VLAN represented by the dotted line, so the traffic segregation engine can be fully eliminated from the LHCCF, as shown in Fig. 7. As all good packets require additional filtering in the private cloud, there is no traffic flowing between public and private clouds over the trusted VLAN represented by the continuous line.

It is clear that in this case, the private cloud needs to process more packets. In such a framework, the CSP cannot draw any additional information from the traffic, except of a fact that part of it is permitted on customer premises. However, the CSP can still maintain a certain knowledge base regarding packets which are explicitly denied in the BFFDDCF, and this gives it a very limited amount of information, as has been stated before. At this point, the amount of information which the CSP can extract by performing traffic eavesdropping and analysis does not differ greatly from that of the regular ISP which the customer is connected to. The original firewall policy cannot be directly read by the CSP or be assumed by performing traffic eavesdropping and analysis. While the first of these two features is provided by the regular Ladon framework, the second is provided by the Ladon Hybrid Cloud only.

CONCLUSIONS

The number of cloud-based services increases every year. The maturity of cloud computing technology encourages organizations to move subsequent types of services, previously impossible to outsource, into the cloud. This includes security services which include firewall services. However, those which have already begun to be widely adopted continue to suffer from information confidentiality and privacy issues as a result of firewall policy outsourcing. While a framework, referred to as Ladon by its authors, preserving the confidentiality of the original firewall policy by introducing BFFDD has been proposed, it has a drawback: There is a risk of firewall de-Anonymization by traffic eavesdropping and analysis. To bypass this issue and limit the amount of information regarding the original firewall structure carried in packet headers, a novel framework introducing the purposefulness of packet decision uncertainty has been proposed in this article as an extension to Ladon. This extension known as the Ladon Hybrid Cloud leverages a hybrid cloud model and performs additional filtering of packets resulting in multiple decisions after passing through BFFDD in a private cloud on customer premises. Additional optimization techniques which help minimize the amount of information carried by particular packets based on the firewall policy type in use have also been proposed. As computational resources of the private cloud are usually limited, an analysis of the Ladon Hybrid Cloud has been performed to check how the framework deals with this. It has been shown in the results of the analysis and confirmed in the results of the experiment that it is possible to control the rate of traffic at the private cloud entrance by selecting appropriate values of BF parameters while knowing basic traffic statistics. It has also been demonstrated that it is possible to find a trade-off between the Ladon Hybrid Cloud privacy level, its congestion probability, and efficiency. The Ladon Hybrid Cloud allows organizations to take back control of privacy by helping them preserve their firewall policy confidentiality when outsourcing firewall services into the cloud. It extends the regular Ladon framework by eliminating its main drawback—the risk of firewall deanonymization by packets eavesdropping and analysis. The Ladon Hybrid Cloud is the final missing part of the puzzle which resolves the key issue of cloud-based firewall services: information confidentiality and privacy.

REFERENCES

1. Furth, B.: Cloud computing fundamentals. In: Furth, B., Escalante, A. (eds.) Handbook of Cloud Computing, pp. 3–20. Springer, New York (2010)
2. SecaaS Working Group: Defined Categories of Service (2011). Cloud Security Aliance (CSA). https://cloudsecurityalliance.org/ wp-content/uploads/2011/09/SecaaS_V1_0 (2011). Accessed 1 Aug 2014
3. AT&T Intellectual Property: Managed Firewall Service NetworkBased. AT&T, Inc. http://www.business.att.com/content/ productbrochures/Network-Based-Firewall (2014). Accessed 1 Aug 2014
4. Virtela Inc: Virtela Enterprise Services Cloud (ESC). Virtela, Inc. http://www.virtela.net/services/virtela-esc/ (2013). Accessed 1 Oct 2013
5. VMware Inc: Business and Financial Benefits of Virtualization. VMware, Inc. http://www.vmware.com/files/pdf/cloud-journey/ VMware-Business-Financial-Benefits-Virtualization-Whitepaper (2011). Accessed 1 Aug (2014)
6. Websence Inc: Seven Criteria for Evaluating Security-as-a-Service (SaaS) Solutions. Websence, Inc. http://www.websense.com/ assets/white-papers/whitepaper-seven-criteria-for-evaluationsecurity-as-a-service-solutions-en (2010). Accessed 1 Aug 2014
7. Zhou, M., Zhang, R., Xie, W., Qian, W. and Zhou, A.: Security and privacy in cloud computing: a survey. In: 6th International Conference on Semantics, Knowledge and Grids, pp. 105–112 (2010)